# 金融诈骗行为特征及其防范机制研究

苏畅

西安财经大学行知学院，陕西西安，710038；

**摘要：**金融诈骗行为借助数字技术与虚拟交易平台持续演变，犯罪链条隐蔽、手法智能、跨域协同，使传统防范体系难以有效应对。本文聚焦金融诈骗的行为逻辑与治理难点，从识别机制滞后、监管协同断裂与公众认知偏弱三个方面剖析风险根源，进而提出跨部门数据联动、金融机构系统风控、风险模型预警、法律制度完善、消费者教育干预及智能反诈平台建设六项对策，意在推动构建动态、高效、协同的金融诈骗防控体系。

**关键词：**金融诈骗；信息联动；风控体系；司法机制；反诈平台

**DOI：**10.64216/3104-9672.25.01.017

## 引言

金融诈骗已突破传统手段范畴，广泛渗透至网络社交、在线支付与虚拟资产交易等多种渠道。随着信息传播加速、金融服务无接触化及公众金融行为数据外泄频发，诈骗团伙构建分工明确、操控精密的犯罪网络，致使金融风险防控难度显著加大。面对犯罪手段智能化、路径复杂化趋势，构建前瞻识别、协同治理与技术驱动并重的风险，识别金融诈骗行为特征、构建应对体系，逐渐成为金融监管的重要任务。

## 1 金融诈骗风险演化的现实背景

信息技术与金融服务深度融合引发金融服务形态剧烈变迁，虚拟账户、移动支付、跨境交易等多维业务场景迅速拓展，为不法分子构建隐匿路径与操控平台提供技术支撑。网络身份认证技术尚未全面覆盖关键支付场景，数据泄露频发助推非法获取身份信息、账号密码、通信记录等敏感数据的黑色产业链蔓延[1]。与此同时，非接触式业务模式弱化传统身份核验手段，导致欺诈风险渗透至业务发起环节。金融诈骗不再局限于简单伪造证件或冒用身份，而是深度嵌入金融活动全流程，掩盖在交易正常逻辑之下，以技术操控、心理诱导、跨境链条等方式实施精准侵害。诈骗团伙结构趋于分工明确，操盘、转账、取现、清洗等环节独立运行，打击难度显著加大。社会舆论场混杂真假信息，诈骗话术紧贴热点舆情与公众心理弱点，使风险认知机制难以及时响应。金融机构间数据壁垒严重，监管机构在情报交换、线索联动与打击协调中面临结构性掣肘。传统金融安全策略多聚焦账户安全、信息加密与交易审计，难以覆盖基于社交工程、虚拟平台与智能算法构建的新型诈骗路径，亟需以系统性视角重构防控框架，推动金融安全治理范式全面升级。

## 2 当前金融诈骗治理面临的主要难点

### 2.1 犯罪手法更新迅速，传统识别机制失效

技术迭代速度驱动诈骗手段持续演化，攻击手段逐步向深度伪装、链式操控与自动化攻击方向推进。诈骗行为开始借助语音合成、深度伪造、人工智能等工具实现精准匹配、实时响应与伪装仿真，导致传统依赖关键词筛查、账户标签与人工核验的识别机制丧失效能。信息披露、合同文本与客户意图呈现高度复杂性，使欺诈信号隐藏于正常业务参数中，标准规则难以识别风险差异。攻击路径不再局限于电话、短信、社交软件，而是深度嵌入虚假平台、虚构项目与假冒投资渠道，通过反复迭代骗术设计对用户信任系统展开系统性干扰。诈骗链条中多个账户环节彼此独立、快速流转，交易碎片化、金额小额化趋势显著，传统反洗钱系统依赖的交易异常判断指标难以捕捉异常流向。风险识别工具普遍滞后于犯罪脚本生成速度，造成前端监控与后端查验之间断层扩大，诈骗交易在识别前已完成资金转移与路径遮蔽，导致识别能力与干预效能同步弱化。

### 2.2 监管协同机制断裂，信息壁垒横亘多端

金融诈骗跨平台、跨区域、跨边界特征突出，单一机构难以独立追踪资金链条与操作路径。当前监管体系多层分立，央行、银保监、公安、网信、电信等机构职能边界交叉，职责划分模糊，信息系统间缺乏标准化接口，数据互通受限，监管协同机制运转缓慢。各监管机构内部多采用闭环自用的数据结构与审查系统，导致诈骗线索在机构间传导不畅，信息滞后严重影响案件合力打击效率。金融机构间出于数据安全、自身合规与业务

壁垒等多重考量，难以实现账户信息、风险评分、黑名单与行为特征的实时共享，诈骗分子往往利用机构信息割裂进行多点突破与身份跳转。跨境资金流转监管存在司法协作难题与技术追踪障碍，诈骗团伙借助海外账户、虚拟币转化与匿名网络隐藏资金去向，极大削弱执法合力。缺乏统一平台承载全国诈骗信息归集与行为分析功能，使监管机构与金融机构难以统一识别风险源头，导致防控措施碎片化、响应滞后化、打击有限化。

### 2.3 公众风险认知偏弱，防范意识普遍滞后

公众在金融素养、诈骗识别与风险防范等方面长期存在认知误区与反应迟钝现象，直接导致诈骗话术易于侵入个人判断体系。多数个体对金融产品复杂性、交易结构合规性与信息安全边界缺乏基本理解，面对高收益诱惑与权威包装难以保持警觉。在新型诈骗话术中，行为操纵策略广泛应用于伪造信任机制、激发情绪恐慌与设置紧迫决策场景，使用户在情绪主导状态下放弃核验与咨询行为。信息传播平台中大量金融广告、投资推荐与账户链接缺乏统一监管标签与信任验证体系，误导信息穿透用户心理防线[2]。高龄群体、青少年群体与低学历用户更易受到冒名信息、熟人语境与技术误导攻击，缺乏识别诈骗特征的经验积累与系统学习。当前防骗教育内容分散、更新迟滞、渠道受限，金融机构在消费者教育方面投入不足，防范知识传播覆盖面低，培训机制针对性差，导致公众难以形成稳定的风险识别行为模式。诈骗防控链条中公众处于首个接触端，认知水平与响应机制直接影响诈骗行为是否得以展开，构建公众金融安全认知屏障迫切性日益凸显。

## 3 构建系统防范体系的应对路径

### 3.1 完善跨部门信息联动

构建覆盖公安、司法、通信、金融监管、电商平台等多部门的信息联动机制，需要统一标准接口与元数据格式，依托国家级金融风险数据平台集成多源异构数据，实现诈骗案件线索、资金流向信息与行为画像的实时共享。监管机构应设立联动指挥中心，配置专职数据分析人员与情报处理系统，形成线索快速响应路径。金融机构需接入统一数据接口，实时上报可疑交易特征与客户行为偏差。跨平台数据共享需建立统一接入规范与权限等级控制体系，在确保数据安全的前提下实现协同流转。对接电信运营商、互联网企业与支付平台的用户行为数据，有助于补强诈骗行为链条信息。通过统一案件编号与风险标识，实现对涉诈账户、涉诈设备与涉诈行为的全域跟踪与节点锁定。司法机关需与监管部门建立案件处理回溯接口，推动诈骗信息同步回流数据中心，持续修正行为特征模型与识别规则集。

### 3.2 强化金融机构内部风控

金融机构应在账户管理系统、支付清算系统与客户行为系统中嵌入高频行为识别模块，对非正常资金流转、快速交易路径与异常登录行为进行动态判别。交易监测系统需接入时间序列分析引擎与规则挖掘引擎，构建基于行为标签与频次阈值的动态判别模型，对账户在短时间内频繁转账、异地操作或非惯常行为模式进行高敏感度识别。风控规则引擎需支持自定义规则配置与模型快速部署，管理人员可依据新型诈骗特征调整识别策略。内部系统需联动客户服务系统，对高风险交易触发自动提醒与人工核验机制。涉诈信号识别后应自动冻结交易流程，并对相关账户进行链式排查。系统需设立多层联动机制，将内部识别结果推送至风险管理中台、客户经营平台与合规检查系统，实现交易级别、客户级别与账户群组级别的全量交叉检视。各业务条线需明确风控责任人配置，确保系统识别结果在业务执行中形成闭环处理路径。

### 3.3 推进事前识别建设

事前识别体系建设需依托风险数据湖与行为评分引擎，融合账户历史行为、设备登录轨迹、资金流转模式与交互行为参数，建立多维行为画像模型，对潜在涉诈客户与高风险交易路径提前设定预警标签。预警模型应引入机器学习算法与深度神经网络结构，动态训练与更新分类边界，提升模型在新型诈骗策略下的识别精度与泛化能力。预警引擎需配置多维权重调节机制，动态调整模型对单因素突变的灵敏度，避免因特征波动误判正常交易。模型部署路径需设定灰名单管理策略，将部分疑似高风险账户设为受限对象，实施额度管控与交易延迟机制，争取识别与干预时间窗口。事前识别体系还应配置风险等级映射接口，与客户信用评分、行为风险指数与历史交易偏离指数联动，形成多维风险聚合标签。系统平台应具备回溯检验模块，持续评估预警模型的误差分布与适用范围，推动模型优化迭代与策略再平衡。

### 3.4 优化法律框架与司法打击精准对接机制

金融诈骗打击环节需以法律制度完备为基础，构建覆盖识别、冻结、打击与追责的全流程司法协同机制。

刑事立法层面应增加针对电信网络诈骗、金融产品欺诈与跨境资金操控行为的专属条文，明确虚拟账户实质认定标准、电子证据适用边界与司法管辖划分机制。最高人民法院与最高人民检察院应发布统一解释文件，对涉诈行为的定性判断、情节认定与量刑标准作出细化指引，消除基层执法与司法尺度差异。检察环节需引入动态证据组合建模方法，综合账户行为轨迹、涉案资金流动图谱与设备关联信息构建电子证据链。公安侦查系统应设立涉诈资金识别模块，对可疑资金路径建立自动溯源模型，并联动金融机构止付系统，在证据阈值满足条件后生成司法冻结请求。跨部门办案过程中应建立电子证据交换平台，支持证据流转记录、调用日志与权限校验，实现司法数据在刑侦、审查起诉与法院裁判三阶段有序流动。涉案财产处置机制应明确权属确认流程与优先赔付顺序，对被害人损失予以资金清算支持。推动国际执法协作框架扩展至加密货币、跨境社交媒体与匿名通信平台，构建应对数字诈骗的司法响应体系。

### 3.5 深耕金融消费者教育与行为干预手段

金融诈骗预防根基在于提升消费者的风险觉察能力与防范行为习惯，金融机构应制定面向不同风险等级用户的教育干预方案，区分账户频次、交易偏好与设备环境特征，构建动态风险画像。高频交易账户应配置智能提示系统，在操作路径中插入图文识别训练与关键术语识别提示，引导用户判断页面真伪与资金去向合法性[3]。面向高风险人群应开展沉浸式防骗教育模拟，将真实诈骗案例嵌入虚拟操作系统，构建认知冲击路径，强化用户记忆回路。在线客服系统应引入行为分析模块，对情绪激动、语言急促与异常操作用户实施人工介入策略，配合短信、语音与 APP 内公告实现立体干预。社区银行、网点与营业厅可设置金融安全知识专区，投放高频诈骗案例短片、折页与风险答题工具，引导老年群体主动参与情景体验。中小学金融素养课程中应引入基础防诈知识与应对路径，引导青少年形成金融风险初步认知系统。金融平台应将用户行为数据反馈至教育内容推荐系统，构建动态内容匹配机制，确保防范知识符合用户使用语境与风险等级。行为干预设计需嵌入操作路径核心节点，在用户点击高风险页面、输入陌生账户或尝试转账异常金额时设置强制等待机制与安全提示环节，配合冻结交易通道形成即时阻断。

### 3.6 构建以科技手段支撑的智能反诈平台

智能反诈平台建设需依托统一数据标准、弹性算法框架与多维建模引擎，整合银行、支付机构、电信运营商与互联网平台数据资源，构建全网联通的风险侦测体系。底层架构应采用分布式数据湖技术，实现结构化数据与非结构化信息并行存储与调用，提升诈骗信息检索速度与覆盖密度。建模层应部署图神经网络构建账户行为链图谱，结合异常点检测算法、集成学习模型与交叉分类器，精准识别伪装账户网络与异常资金集散点。识别模块应内嵌强化学习算法，对反侦察行为进行动态适应，形成以风险行为反馈驱动模型优化的自学习系统。模型部署应覆盖终端 APP、后台风控与管理端中台系统，在交易发起、账户操作与消息推送等节点同步运行预警模块。数据可视化平台应展示诈骗热力分布图、行为链断点图与涉诈路径转移图，辅助监管机构与金融企业进行区域治理与结构决策。系统还需配置智能响应机制，当置信度超过阈值时自动启动账户冻结、交易拦截与风险分级通报流程，实现毫秒级响应能力。平台安全结构需设定分级授权与访问审计模块，确保模型调用行为可回溯、接口权限可控、数据调阅合规。全国范围内应设立统一反诈算法共享仓库与模型比测机制，推动高效模型迭代与技术资源统一调度，形成覆盖事前监测、事中阻断与事后追踪的科技反诈闭环系统。

## 4 结束语

金融诈骗防控工作需打破条块分割格局，推动信息共享机制贯通全链条治理逻辑，重塑以科技为核心驱动、法治为刚性约束、公众为主体屏障的立体防控系统，助力金融秩序稳定与公共安全体系迭代升级。

## 参考文献

[1]本刊编辑部.防范利用新技术进行电信诈骗守护消费者资金安全——金融消费者权益保护典型案例四则[J].中国银行业,2025,(01):91-94.
[2]黄秦,肖珍珍.电信网络诈骗主要类型以及金融机构防范措施[J].现代商贸工业,2024,(23):202-204.
[3]林红梅,王优玲,屈婷.老年人如何防范金融消费诈骗[J].湖南农业,2024,(10):47-48.

作者简介：苏畅（2002.08—），男，汉族，内蒙古自治区鄂尔多斯市人，大学本科，研究方向：金融诈骗特征、多主体防范机制。